国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2017 年 04 月 10 日-2017 年 04 月 16 日 **2017 年第 16 期**

本周漏洞态势研判情况

本周信息安全漏洞威胁整体评价级别为**高**。

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 209 个，其中高危漏洞 88 个、中危漏洞 114 个、低危漏洞 7 个。漏洞平均分值为 6.27。本周收录的漏洞中，涉及 0day 漏洞 50 个（占 24%），其中互联网上出现“Microsoft Windows 本地权限提升漏洞（CNVD-2017-04425）、Joomla com_kide 插件'view'参数 SQL 注入漏洞”零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 597 个，与上周（641 个）环比下降 7%。此外，本周由于互联网上披露了方程式黑客组织使用的多个漏洞利用工具，使得 Windows 服务器主机以及一些应用广泛的邮件服务器出现大规模攻击威胁，因此本周整体评价级别为高。

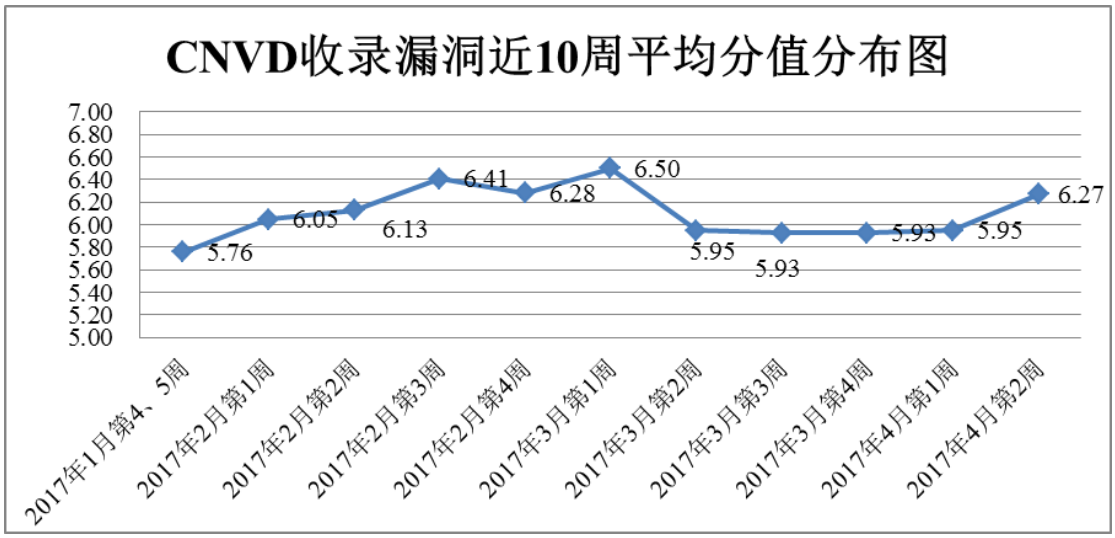

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 15 家成员单位、合作伙伴及企业用户、个人用户报送了本周收录的全部 209 个漏洞。报送情况如表 1 所示。其中，安天实验室、H3C、启明星辰、中国电信集团

系统集成有限责任公司等单位报送数量较多。漏洞盒子、安徽新华博信息技术股份有限公司、江苏君立华域信息安全技术股份有限公司、杭州朔方信息技术有限公司、广西鑫瀚科技有限公司、山东安云信息技术有限公司、清远职业技术学院、北京山石网科信息技术有限公司、河北网信智安信息技术有限公司及其他个人白帽子向 CNVD 提交了 597 个以事件型漏洞为主的原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
360 网神	284	284
安天实验室	128	0
H3C	110	0
启明星辰	104	1
中国电信集团系统集成有限责任公司	83	0
华为技术有限公司	75	0
绿盟科技	71	0
天融信	63	1
安全狗	29	2
杭州安恒信息技术有限公司	28	0
阿里云计算有限公司	12	0
恒安嘉新	11	0
北京数字观星科技有限公司	5	0
深圳市深信服电子科技有限公司	1	1
西安四叶草信息技术有限公司	1	1
漏洞盒子	127	127
安徽新华博信息技术股份有限公司	16	16
江苏君立华域信息安全技术股份有限公司	5	5
杭州朔方信息技术有	5	5

限公司		
广西鑫瀚科技有限公司	4	4
山东安云信息技术有限公司	4	4
清远职业技术学院	4	4
北京山石网科信息技术有限公司	3	3
河北网信智安信息技术有限公司	1	1
CNCERT 湖南分中心	7	7
CNCERT 广东分中心	5	5
CNCERT 宁夏分中心	2	2
CNCERT 上海分中心	2	2
CNCERT 新疆分中心	1	1
CNCERT 内蒙古分中心	1	1
CNCERT 吉林分中心	1	1
CNCERT 河北分中心	1	1
CNCERT 北京分中心	1	1
个人	117	117
报送总计	1312	597
录入总计	209（去重）	597

表 1 漏洞报送情况统计表

本周漏洞按类型和厂商统计

本周，CNVD 收录了 209 个漏洞。其中应用程序漏洞 122 个，web 应用漏洞 51 个，网络设备漏洞 16 个，安全产品漏洞 12 个，操作系统漏洞 8 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	122
web 应用漏洞	51

网络设备漏洞	16
安全产品漏洞	12
操作系统漏洞	8

表 2 漏洞按影响类型统计表

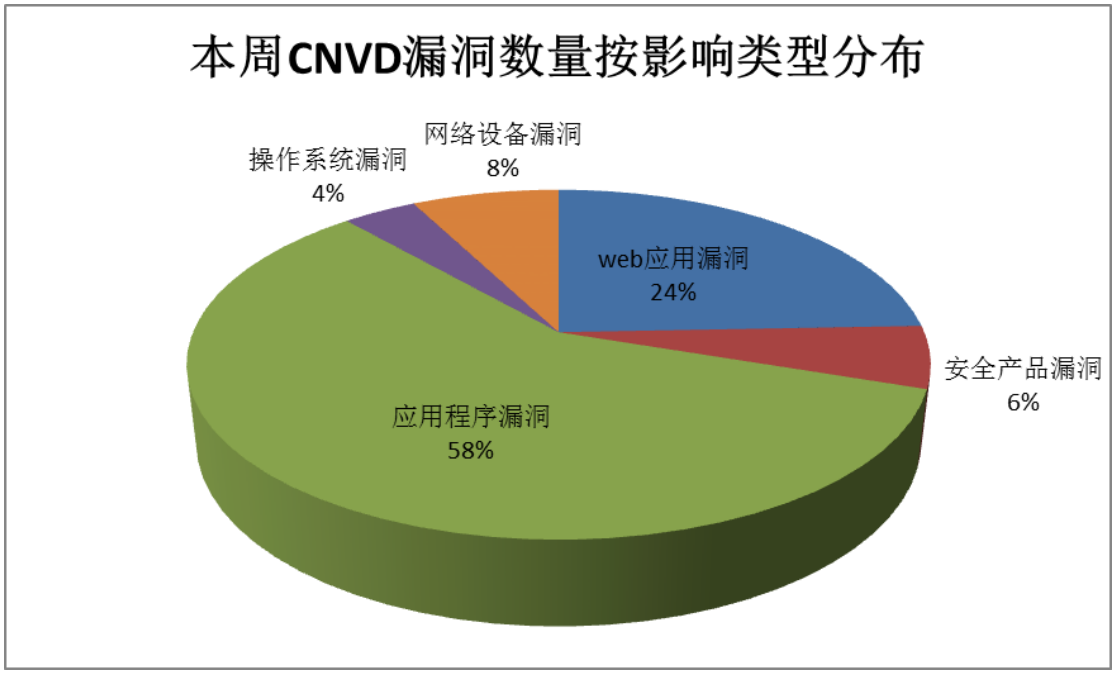

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Mozilla、Joomla、ImageMagick 等多家厂商的产品，部分漏洞数量按厂商统计如表 3 所示。

序号	厂商（产品）	漏洞数量	所占比例
1	Mozilla	20	10%
2	Joomla	15	7%
3	ImageMagick	11	5%
4	Adobe	10	5%
5	PoDoFo	10	5%
6	Ntp	9	4%
7	Microsoft	7	3%
8	GNU	5	2%
9	Cisco	4	2%
10	其他	118	57%

表 3 漏洞产品涉及厂商分布统计表

本周行业漏洞收录情况

本周，CNVD 收录了 7 个电信行业漏洞，2 个移动互联网行业漏洞，2 个工控系统行业漏洞（如下图所示）。其中，“Android Qualcomm Wi-Fi 权限提升漏洞”的综合评级为“高危”。相关厂商已经发布了上述漏洞的修补程序，请参照 CNVD 相关行业漏洞库链接。

电信行业漏洞链接：http://telecom.cnvd.org.cn/

移动互联网行业漏洞链接：http://mi.cnvd.org.cn/

工控系统行业漏洞链接：http://ics.cnvd.org.cn/

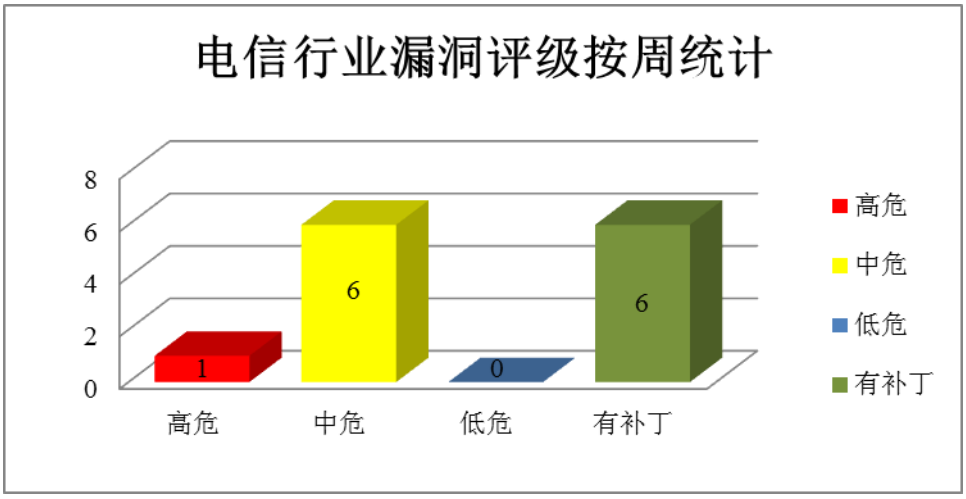

图 3 电信行业漏洞统计

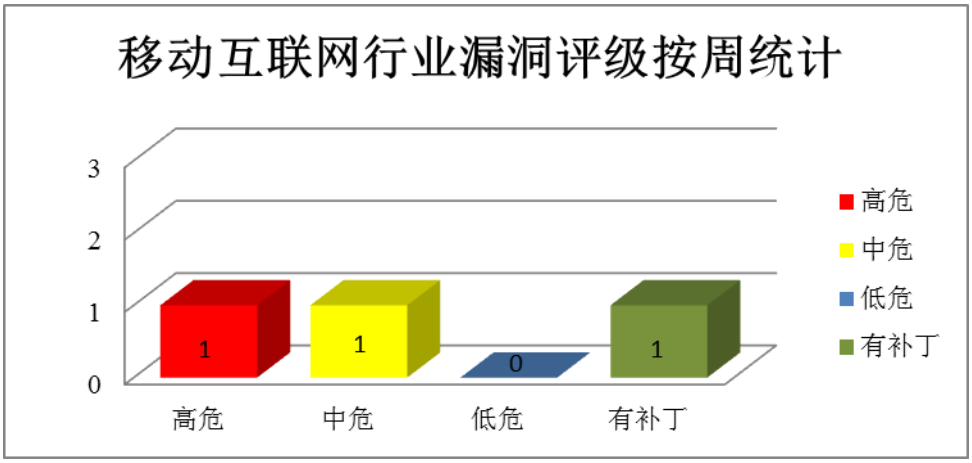

图 4 移动互联网行业漏洞统计

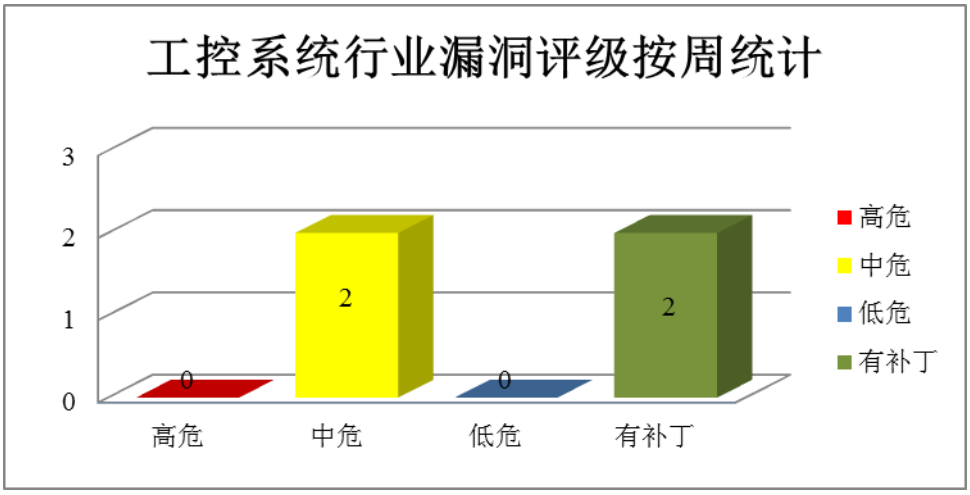

图 5 工控系统行业漏洞统计

本周重要漏洞安全告警

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、Adobe 产品安全漏洞

Adobe Flash Player 是美国 Adobe 公司开发的一款广泛使用的、专有的多媒体程序播放器。Adobe Acrobat Reader 是用于打开和使用在 Adobe Acrobat 中创建的 Adobe PDF 的工具。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Acrobat 和 Reader 内存破坏漏洞（CNVD-2017-04423）、Adobe Flash Player 代码执行漏洞（CNVD-2017-04422、CNVD-2017-04298、CNVD-2017-04299、CNVD-2017-04301、CNVD-2017-04300、CNVD-2017-04303）、Adobe Flash Player 缓冲区溢出漏洞（CNVD-2017-04304）。上述漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2017-04423
http://www.cnvd.org.cn/flaw/show/CNVD-2017-04422
http://www.cnvd.org.cn/flaw/show/CNVD-2017-04298
http://www.cnvd.org.cn/flaw/show/CNVD-2017-04299
http://www.cnvd.org.cn/flaw/show/CNVD-2017-04301
http://www.cnvd.org.cn/flaw/show/CNVD-2017-04300
http://www.cnvd.org.cn/flaw/show/CNVD-2017-04303
http://www.cnvd.org.cn/flaw/show/CNVD-2017-04304

2、NTP 产品安全漏洞

NTP 是网络时间协议(Network Time Protocol)，是用来同步网络中各个计算机的时间的协议。本周，上述产品被披露存在拒绝服务和缓冲区溢出漏洞，攻击者可利用漏洞发起拒绝服务攻击或执行任意代码。

CNVD 收录的相关漏洞包括：NTP 本地拒绝服务漏洞（CNVD-2017-04410、CNVD-2017-04411、CNVD-2017-04413）、NTP 本地栈缓冲区溢出漏洞、NTP 缓冲区溢出漏洞（CNVD-2017-04230）、NTP 拒绝服务漏洞（CNVD-2017-04414、CNVD-2017-04415、CNVD-2017-04247）。其中“NTP 本地拒绝服务漏洞（CNVD-2017-04411）、NTP 拒绝服务漏洞（CNVD-2017-04247）”的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2017-04410
http://www.cnvd.org.cn/flaw/show/CNVD-2017-04411
http://www.cnvd.org.cn/flaw/show/CNVD-2017-04413
http://www.cnvd.org.cn/flaw/show/CNVD-2017-04412
http://www.cnvd.org.cn/flaw/show/CNVD-2017-04230
http://www.cnvd.org.cn/flaw/show/CNVD-2017-04414
http://www.cnvd.org.cn/flaw/show/CNVD-2017-04415
http://www.cnvd.org.cn/flaw/show/CNVD-2017-04247

3、Microsoft 产品安全漏洞

Microsoft Windows 是美国微软（Microsoft）公司发布的一系列操作系统。PDF library 是其中的一个 PDF 库。IIS Server 是其中的一个运行于其中的互联网基本服务。Microsoft Office 是一款微软开发的流行的办公软件套件。Microsoft Edge 是一款 Web 浏览器。Microsoft Internet Explorer 是一款流行的 WEB 浏览器。Microsoft Exchange Server 是一款微软开发的邮件服务程序。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升特权、执行任意代码和执行跨站脚本攻击等。

CNVD 收录的相关漏洞包括：Microsoft Office Word OLE 对象代码执行漏洞、Microsoft Windows 本地权限提升漏洞（CNVD-2017-04425）、Microsoft Windows PDF 内存破坏漏洞、Microsoft Windows Server Message Block 任意代码执行漏洞、Microsoft Internet 信息服务器（IIS）Web 跨站脚本漏洞、Microsoft Exchange Server 远程特权提升漏洞、Microsoft Internet Explorer 和 Edge 欺骗漏洞。除“Microsoft Internet 信息服务器（IIS）Web 跨站脚本漏洞、Microsoft Exchange Server 远程特权提升漏洞、Microsoft Internet Explorer 和 Edge 欺骗漏洞”外，其余漏洞的综合评级为“高危”。目前，厂商已经发布了除“Microsoft Windows 本地权限提升漏洞（CNVD-2017-04425）”外漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2017-04293
http://www.cnvd.org.cn/flaw/show/CNVD-2017-04425
http://www.cnvd.org.cn/flaw/show/CNVD-2017-04244
http://www.cnvd.org.cn/flaw/show/CNVD-2017-04243
http://www.cnvd.org.cn/flaw/show/CNVD-2017-04245

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04249

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04248

4、Mozilla 产品安全漏洞

Mozilla Firefox 是美国 Mozilla 基金会开发的一款开源 Web 浏览器。Thunderbird 是由 Mozilla 浏览器的邮件功能部件所改造的邮件工具。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制执行未授权操作，获取敏感信息，执行任意脚本代码等。

CNVD 收录的相关漏洞包括：Mozilla Firefox MFSA 存在多个漏洞、Mozilla Firefox MFSA 存在多个漏洞（CNVD-2017-04171、CNVD-2017-04172）、Mozilla Firefox MFSA 内存错误引用漏洞、Mozilla Firefox 内存错误引用漏洞（CNVD-2017-04176）、Mozilla Firefox/Thunderbird 存在多个漏洞、Mozilla Firefox/Thunderbird 存在多个漏洞（CNVD-2017-04251、CNVD-2017-04250）。除“Mozilla Firefox/Thunderbird 存在多个漏洞（CNVD-2017-04250）”外，其余漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2017-04173

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04171

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04172

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04175

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04176

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04253

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04251

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04250

5、多个 Avira 产品 DLL 加载本地代码注入漏洞

Avira Total Security Suite 等都是德国小红伞（Avira）公司的杀毒软件。本周，Avira 被披露存在 DLL 加载本地代码注入漏洞，本地攻击者可利用此漏洞在受影响程序中运行的系统的上下文中执行任意代码，获取受影响程序的完全控制权限。目前，互联网上已经出现了针对该漏洞的攻击代码，厂商尚未发布漏洞修补程序。CNVD 提醒广大用户随时关注厂商主页，以获取最新版本。

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2016-04262

更多高危漏洞如表 4 所示，详细信息可根据 CNVD 编号，在 CNVD 官网进行查询。

参考链接:http://www.cnvd.org.cn/flaw/list.htm

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2017-04275	Moodle SQL 注入漏洞（CNVD-2017-04275）	高	用户可联系供应商获得补丁信息：https://moodle.org/

CNVD-2017-04295	ImageMagick 函数拒绝服务漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：http://www.imagemagick.org
CNVD-2017-04307	OxygenOS 代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://securityresear.ch/2017/02/08/oneplus3-bootloader-vulns/
CNVD-2017-04308	OxygenOS 权限提升漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://securityresear.ch/2017/02/08/oneplus3-bootloader-vulns/
CNVD-2017-04312	Zammad 安全绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://zammad.com/de/news/security-advisory-zaa-2017-01
CNVD-2017-04305	Zammad 安全绕过漏洞（CNVD-2017-04305）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://zammad.com/de/news/security-advisory-zaa-2017-01
CNVD-2017-04313	Android Qualcomm Wi-Fi 权限提升漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/security/bulletin/2017-03-01.html
CNVD-2017-04334	phplist SQL 注入漏洞（CNVD-2017-04334）	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://www.phplist.org/
CNVD-2017-04357	Commvault Edge 栈缓冲区溢出漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：http://kb.commvault.com/article/SEC0013
CNVD-2017-04454	FortiClient SSLVPN 特权提升漏洞	高	用户可联系供应商获得补丁信息：https://www.fortinet.com/

表 4 部分重要高危漏洞列表

小结：本周，Adobe 被披露存在多个漏洞，攻击者可利用漏洞执行任意代码。此外，NTP、Microsoft、Mozilla 等多款产品被披露存在多个漏洞，攻击者利用漏洞可执行任意代码、绕过安全限制、提升权限或发起拒绝服务攻击等。另外，Avira 被披露存在 DLL 加载本地代码注入漏洞，本地攻击者可利用此漏洞在受影响程序中运行的系统的上下文中执行任意代码，获取受影响程序的完全控制权限。建议相关用户随时关注上述厂商主页，及时获取修复补丁或解决方案。

本周漏洞要闻速递

1. Linux 内核 ipv4/udp.c 远程任意代码执行(CVE-2016-10229)

Linux kernel 是美国 Linux 基金会发布的操作系统 Linux 所使用的内核。Linux kernel 4.5 之前的版本中的 udp.c 文件存在安全漏洞，Linux 内核中的 udp.c 允许远程攻击者通过 UDP 流量执行任意代码，这些流量会在执行具有 MSG_PEEK 标志的 recv 系统调用时触发不安全的第二次校验和计算，远程攻击者可精心构造数据执行任意代码，进一步导致本地提权，属于高危漏洞。但由于现实情况中，基于 UDP 协议的服务时 MSG_PEEK 标志在实际使用的情况较少，受该远程命令执行漏洞危害影响群体范围有限。

参考链接：http://www.freebuf.com/vuls/131907.html

2. Word 曝 0day 漏洞：无需启用宏，打开文档就自动安装恶意程序

研究员表示，他们在一封邮件中发现了恶意 Word 文档附件，该文件包含 OLE2link 对象。一旦打开文件，文件中的利用代码就会执行，随后连接到一台由攻击者所控制的远程服务器，并从服务器上下载伪装成 RFT 文档的 HTML 应用文件（HTA）。HTA 文件自动执行，攻击者就能实现目标设备之上的任意代码执行了，随后开始从”其他知名恶意软件家族“下载额外的 payload，这些 payload 感染目标 PC，并关闭该恶意 Word 文件。通过 Office Protected View（受保护视图）特性查看这种恶意文档就可让攻击失效，因此我们建议 Windows 用户在查看 Office 文档时开启此特性。

参考链接：http://www.freebuf.com/vuls/131586.html

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

关于 CNCERT

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，为非政府非盈利的网络安全技术中心，是我国网络安全应急体系的核心协调机构。

作为国家级应急中心，CNCERT 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82990999